TILS 1065

advies aan b&w

GEMEENTE WEERT

Sector	: Inwoners		Openbaar: ☑
Afdeling	: Werk, Inkomen en Zorgverlening		Niet openbaar: ☐
Zaaknummer(s) ingekomen stuk(ken)	:		Kabinet: ☐
Behandelend medewerk(st)er	: Ümügül Tasim-Mustafa en: Kees Joosten	Tel.: (0495) 57 58 98	
Portefeuillehouder(s)	: A.A.M.M. Heijmans		Nummer B&W-advies: BW-008288

ONDERWERP

Handboek Informatiebeveiliging WIZ Security Officer Suwinet

ADVIES

1. Vaststellen van het Handboek Informatiebeveiliging WIZ.
2. Benoemen van Security Officer Suwinet dhr. Harrie van Helvoort, Adviseur Informatievoorziening.

TOELICHTING

Relatie met vorig voorstel:
Collegebesluit van 28 januari 2014 (BW-006825), Vaststellen van het Handboek Informatiebeveiliging WIZ.

Algemeen:
Op 28 januari 2014 heeft uw college het handboek Informatiebeveiliging WIZ vastgesteld. Op 14 juli 2014 heeft de Inspectie van het ministerie SZW de gemeente Weert geselecteerd voor de steekproef Veilig gebruik Suwinet. Dit onderzoek heeft plaatsgevonden op verzoek van de staatssecretaris met als doel om vast te stellen of de gemeenten voldoen aan de eisen die worden gesteld aan de beveiliging van persoonsgegevens die worden uitgewisseld binnen Suwinet.

		S		B	W HL	W E	W PS	W GG
Weert, 3 april 2015 De directeur,			akkoord					
			bespreken					
		Behandeling uiterlijk in college van 14 april 2015						

In te vullen door het B&W secretariaat:

☐ Akkoord
☐ Akkoord met tekstuele aanpassing door portefeuillehouder
☐ Anders, nl.:

☐ Niet akkoord
☐ Gewijzigde versie

☐ A-stuk
☐ B-stuk
☐ C-stuk

Beslissing d.d.: Akkoord met advies 14 APR. 2015 Nummer: 8

De secretaris,

Totaal aantal pagina's: 2
Pagina 1

Argumenten:
Op 27 januari 2015 heeft de Inspectie SZW het conceptverslag van bevindingen onderzoek Veilig gebruik Suwinet verstuurd naar uw college. Uit het conceptverslag van bevindingen bleek dat de gemeente Weert op 4 van de 7 punten voldeed, echter op 3 punten niet.
Op basis van het conceptverslag van bevindingen heeft uw college op 9 februari 2015 een reactie gestuurd waarin aangegeven wordt dat uw college op de drie onderdelen waarin we nog niet voldeden de aanbevelingen van de Inspectie overneemt (zie Bijlage 2).

In de oude structuur was het afdelingshoofd Werk, Inkomen en Zorgverlening ook de Security Officer van Suwinet. Om belangen verstrengeling te voorkomen stellen we voor dat dhr. Harrie van Helvoort, Adviseur Informatievoorziening te benoemen als security officer Suwinet.
Op basis van de aanbevelingen van de inspectie is het Handboek Informatiebeveiliging WIZ aangepast.

Kanttekeningen:
N.v.t.

JURIDISCHE GEVOLGEN (o.a. FATALE TERMIJNEN/HANDHAVING)

N.v.t.

FINANCIËLE EN PERSONELE GEVOLGEN

Dit voorstel heeft geen financiële en personele gevolgen.

COMMUNICATIE/PARTICIPATIE

Voor wie is dit advies van belang?:
- Raadsleden

Nadere specificatie: De raadsleden worden middels de TILS-lijst geïnformeerd over dit besluit.

Geadviseerd wordt de volgende communicatie-instrumenten te gebruiken:
- TILS-lijst

Nadere specificatie:

Geadviseerd wordt de volgende participatie-instrumenten te gebruiken:
- Niet van toepassing

OVERLEG GEVOERD MET

Intern:
Kees Joosten, hoofd afdeling WIZ
Bertus Brinkman, directeur Bedrijfsvoering

Extern:

BIJLAGEN

Openbaar:
Bijlage 1: Handboek Informatiebeveiliging WIZ
Bijlage 2: Reactie college n.a.v. brief Inspectie SZW

Niet-openbaar:
Niet van toepassing

Informatiebeveiligingsplan

*

De beveiliging van gegevens bij de

Sector Inwoners Gemeente Weert
Afdeling Werk, Inkomen en Zorg

Weert,
geactualiseerd maart 2015 versie 3.0
Oorspronkelijke versie december 2012, versie 1.0

Inhoud

Hoofdstuk 1. Inleiding

1.1 Doel van informatiebeveiliging

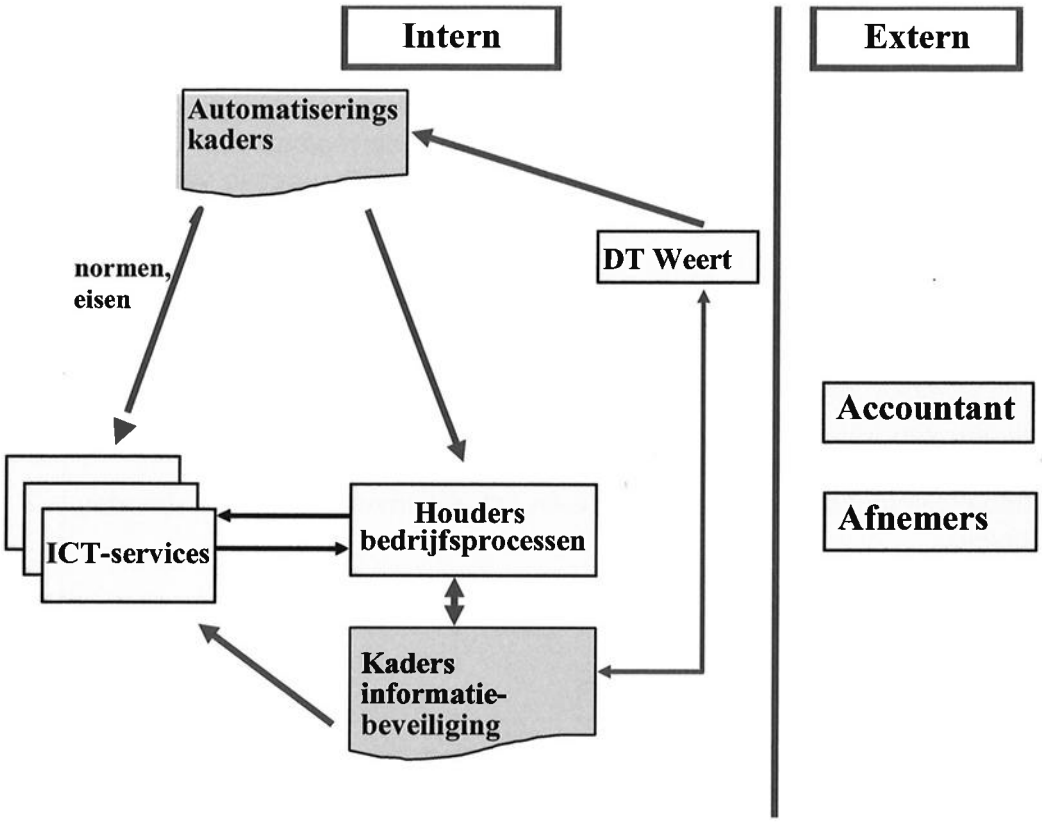
De primaire en ondersteunende processen van de afdeling WIZ, (Werk, Inkomen & Zorg) zijn in hoge mate afhankelijk van een adequate informatievoorziening en betrouwbare informatiesystemen.

Het toenemende gebruik van datacommunicatie en geautomatiseerde systemen leidt tot een grote afhankelijkheid en kwetsbaarheid van de bedrijfsvoering binnen de gemeente Weert. De risico's die hiermee samenhangen, kunnen aanzienlijk zijn en kunnen een bedreiging vormen voor de vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening en daarmee indirect voor het imago en dus de continuïteit van de gemeente Weert.

Gelet op de mogelijke impact van verstoringen op de continuïteit van de bedrijfsvoering berust de eindverantwoordelijkheid voor het beleid betreffende de beveiliging en de interne controle van de geautomatiseerde informatievoorziening bij het DT (DirectieTeam van de gemeente Weert).
Informatie wordt in elk proces binnen de gemeente gebruikt en dus zijn alle sectoren en afdelingen, als houder van de door hun gebruikte informatiesystemen, verantwoordelijk voor de uitvoering ervan.

Het DirectieTeam (DT) stelt de kaders van het informatiebeveiligingsbeleid vast,
de houders van de bedrijfsprocessen werken volgens deze beleidsuitgangspunten en
ICT-services ondersteunt de afdelingen en sectoren.
ICT-services is de houder van de overeengekomen technische infrastructuur, waaronder inbegrepen de infrastructurele beveiligingsmiddelen.
(Hierna schematisch weergegeven)

Een basisniveau van gemeenschappelijke beveiligingseisen en maatregelen is het begin van een systematische beveiligingsaanpak. Dit basis beveiligingsniveau dient voor de gehele organisatie toepasbaar en geldig te zijn. Het kan hierbij om elementaire zaken gaan zoals toegangsbeveiliging (toegang binnen en buiten openingstijden / kantooruren), autorisatieschema's, functiescheiding, het onderbrengen van back-ups in een ander gebouw en virusprotectie.



Dit *informatiebeveiligingsplan* is er op gericht om de betrouwbaarheid, de integriteit en de vertrouwelijkheid van de (geautomatiseerde) gegevensuitwisseling binnen onze afdeling (Werk, Inkomen & Zorg) te waarborgen. Om de beheersbare en betrouwbare informatievoorziening te realiseren is het van belang een aantal gemeenschappelijke uitgangspunten te hanteren en deze uit te dragen.

1.2 Lijnmanagement

Informatiebeveiliging zal in de hele organisatie geborgd moeten zijn. Omdat binnen de Gemeente Weert sprake is van integraal management door de afdelingshoofden, zijn deze verantwoordelijk voor de uitvoering van het beveiligingsbeleid. Vergroten van de bewustwording is een belangrijke taak.

1.3 Definitie informatiebeveiliging

In deze paragraaf wordt kort aangegeven wat als definitie van informatiebeveiliging wordt gehanteerd.

Onder informatiebeveiliging wordt verstaan:
"Het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de betrouwbaarheid van het informatievoorzieningproces".

"Betrouwbaarheid" is de overkoepelende term voor *beschikbaarheid* (continuïteit, responstijd), *integriteit* (juistheid, volledigheid, tijdigheid, geoorloofdheid) en *vertrouwelijkheid* (exclusiviteit).
Met het inzichtelijk maken en het nemen van maatregelen wordt aangegeven in welke mate de gemeente Weert kan vertrouwen op een informatiesysteem voor haar informatievoorziening. Dit betreft zowel de technische, de organisatorische, als de menselijke aspecten.

1.4 Beveiligingsbeleid

In het beleidsdocument "informatiebeveiliging van geautomatiseerde systemen binnen de gemeente Weert" van 05 november 2002, zijn eisen en maatregelen voor de gehele organisatie vastgesteld. In deze versie is vastgehouden aan de indeling van de Code voor Informatiebeveiliging.

Dit voor de gemeente Weert opgestelde Informatiebeveiligingsbeleid is niet meer actueel. De uitgangspunten fungeren wel als leidraad voor dit beveiligingsplan.

De staf van de afdeling Werk, Inkomen en Zorg maakt met dit beveiligingsplan aantoonbaar dat zij het belang van informatiebeveiliging ondersteunt. Hiervoor wacht men niet totdat het concernbrede informatiebeveiligingsbeleid geactualiseerd is.
Dit informatiebeveiligingsplan is een concrete en actuele invulling van het destijds opgestelde beleid.

Hoofdstuk 2. Wetgeving

2.1 Wet Bescherming Persoonsgegevens

De Wet Bescherming Persoonsgegevens (Wbp) stelt dat persoonsgegevens alleen voor welbepaalde uitdrukkelijke omschreven en gerechtvaardigde doeleinden mogen worden verkregen.
De Wbp heeft tot doel het reguleren van de omgang met persoonsgegevens en stelt regels en voorwaarden aan het verwerken van persoonsgegevens ter bescherming van de privacy van iedereen van wie gegevens worden verwerkt.

Beveiliging van persoonsgegevens is een van de speerpunten van het handhavingsbeleid van het CBP*. Het CBP houdt toezicht op de naleving van de Wet bescherming persoonsgegevens (Wbp). Artikel 13 van de Wbp eist dat bedrijven en overheden die persoonsgegevens verwerken, 'passende technische en organisatorische maatregelen' nemen om persoonsgegevens te beveiligen

Als gevolg van de Wbp moeten persoonsgegevens in overeenstemming met de Wbp en op behoorlijke en zorgvuldige wijze worden verwerkt. Op hoofdlijnen betekent dit:

1 persoonsgegevens mogen slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld;
2 voor de verwerking dient een van de in de Wbp genoemde rechtvaardigingsgronden te bestaan;
3 slechts onder bepaalde voorwaarden mogen persoonsgegevens voor andere doeleinden worden gebruikt dan waarvoor ze zijn verzameld; zijn;
4 de organisatie treft de nodige maatregelen zodat de persoonsgegevens, gelet op het doel waarvoor ze worden verwerkt, juist en nauwkeurig zijn;
5 de organisatie legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking; de verantwoordelijke dient er tevens voor te zorgen dat ook de bewerker voldoende waarborgen biedt met betrekking tot technische en organisatorische beveiliging;
6 de organisatie informeert de betrokkene over de verwerking van zijn persoonsgegevens en biedt zij de betrokkene de gelegenheid tot inzage in zijn persoonsgegevens.

Eén van de verplichtingen van de Wbp is dat in principe alle verwerkingen van persoonsgegevens moeten worden gemeld bij het College bescherming persoonsgegevens.

Voor de afdeling Werk, Inkomen en Zorg zijn de volgende verwerkingen gemeld:

- Uitkeringsadmininstratie (m.b.v. Civision SAM)
- Suwinet- Inkijk
- Frauderegistratie (m.b.v. liaan)

De rol van Security Officer wordt binnen de afdeling Werk, Inkomen en Zorg vervuld door dhr. Harrie van Helvoirt, medewerker sector Bedrijfsvoering, afdeling Personeel Informatie Facilitair. De Security Officer zal 2 keer per jaar de beveiliging rondom Suwinet controleren en beoordelen en rapporteren aan het hoogste management.

2.2 SUWI Wet- en regelgeving en de WWB

Ook in de wetgeving in de sociale zekerheidssector zijn bepalingen opgenomen die tot doel hebben de persoonlijke levenssfeer van betrokkenen te beschermen.
Voor onze dienst is dit onder andere de Wet Structuur uitvoering werk en inkomen (wet SUWI), het Besluit en de Regeling SUWI.

Uit de SUWI regelgeving vloeien doel en taken van de sociale dienst/afdeling sociale zaken en de overige SUWI partijen voort. De sectorale wetgeving regelt onder meer de informatievoorziening van de SUWI-organisaties onderling en aan derden. Daarbij is bepaald dat de gegevensstromen tussen de SUWI-organisaties via het SUWINET verlopen. Gegevensstromen waarin de SUWI regelgeving niet voorziet zal, zonder goedkeuring van de Minister, niet plaatsvinden. Voor zover in de wet SUWI niet van de Wbp wordt afgeweken, geldt de Wbp.

Vanaf 2004 dient iedere gemeente in overeenstemming met Artikel 6.4, Regeling SUWI, in een beveiligingsplan aan te geven op welke wijze zij invulling geeft aan de beveiliging van de gegevensuitwisseling in het kader van SUWI.

De inspectie SZW kan op basis van bevindingen van Divosa* en de VNG onderzoek doen naar de beveiliging van SUWINET. Als blijkt dat de gemeente niet voldoet aan de eisen van de Wbp kan het College Bescherming Persoonsgegevens, volgens Artikel 60 Wbp, een dwangsom opleggen.
Recentelijk heeft de inspectie SZW in het rapport "de burger bediend in 2013", nog geconstateerd dat gemeenten onvoldoende adequate maatregelen hebben getroffen om de beveiliging van SUWINET op orde te brengen.

Daarnaast is de Wet Werk en Bijstand (WWB) relevant. In de WWB is een aparte paragraaf opgenomen (6.6 gegevensuitwisseling) over de regels die van toepassing zijn bij de uitwisseling van persoonsgegevens. Deze paragraaf kan als volgt op hoofdlijnen worden geschetst:

1 werkgevers hebben een informatieplicht om inlichtingen te verstrekken over de aanvrager van een uitkering of een uitkeringsgerechtigde betreffende omstandigheden die noodzakelijk zijn voor de uitvoering van de WWB;
2 diverse instanties, zoals het UWV, College voor zorgverzekeringen, pensioenfondsen, etc. hebben een informatieplicht naar de sociale dienst/afdeling sociale zaken indien noodzakelijk voor de uitvoering van de WWB;
3 medewerkers die met persoonsgegevens in aanraking komen hebben een geheimhoudingsplicht, tenzij het voor de uitvoering van de WWB noodzakelijk is deze persoonsgegevens te verstrekken aan anderen.
4 de gemeente heeft een inlichtingenverplichting binnen gestelde regels ten aanzien van diverse instellingen, zoals het UWV, de Sociale verzekeringsbank, de Belastingdienst, overige gemeenten etc. Voor de verstrekking van gegevens tussen instanties wordt gebruik gemaakt van het BSN-nummer.

2.3 Overige wetgeving

Naast de wetgeving in de sociale zekerheidssector en de Wbp geldt er diverse andere wet- en regelgeving, zoals de Archiefwet.

Verdere wetgeving die in dit kader relevant kan zijn:

De Wet WEU, die vier jaar geleden van kracht werd, stelt dat een aantal gegevens in principe niet meerdere malen mag worden uitgevraagd door organisaties in het werk- en inkomendomein.

Substitutiewet digitale/fysieke documenten.
Er mag pas afscheid worden genomen van de papieren informatie als er voldoende garanties bestaan over de kwaliteit van de digitale informatie.
Ook voor de digitale informatie zullen afspraken moeten worden gemaakt over toegankelijkheid, beschikbaarheid, integriteit en authenticiteit van de informatie.

Wet SUWI (Wet Structuur Uitvoeringsorganisatie Werk en Inkomen).
Met deze wet is het mogelijk gemaakt dat UWV, SVB en de gemeentelijke sociale diensten digitaal gegevens met elkaar gingen uitwisselen.

Per 1 maart 2013 zijn de richtsnoeren beveiliging persoonsgegevens van het CBP in werking getreden.

Hoofdstuk 3. Reikwijdte

3.1 Applicaties

Hierbij maken we onderscheid tussen de SUWI applicatie en de overige applicaties waarmee de afdeling WIZ werkt zoals Civision SAM, Liaan SR, Liaan herberekenen, Liaan Inlichtingenburo.

SUWI applicatie
De omgeving waarbinnen de normen geplaatst moet worden, wordt gedefinieerd door de volgende functies:
SUWINET Inkijk
direct en snel ophalen van gegevens op een gestandaardiseerde wijze, op basis van webtechnologie, via SUWINET. Inclusief de informatie van de VIP Verificatie Informatie Persoonsbewijzen, dan wel het inlichtingenbureau.

Voor wie is Suwinet- Inkijk?
Suwinet- Inkijk is voor overheidsorganisaties die, voor het uitvoeren van hun wettelijke taken, gegevens van burgers en bedrijven nodig hebben. Suwinet- Inkijk maakt gebruik van geregistreerde gegevens van organisaties die zijn aangesloten op SUWINET.

Dagelijks gebruiken 25.000 professionals Suwinet- Inkijk.
Elke maand worden gegevens van ruim 600.000 Nederlanders opgevraagd

Suwinet- Inkijk is dus niet vrijblijvend. Aan Suwinet- Inkijk zijn regels verbonden.

Toegangsbeveiliging
Toegangsbeveiliging is een belangrijk onderdeel van Suwinet- Inkijk, niet alleen vanuit oogpunt van privacy, maar ook in relatie tot continuïteit is het van groot belang dat zeker kan worden gesteld dat alleen geautoriseerde gebruikers toegang hebben tot de SUWI-

gegevens. De toegang tot Suwinet- Inkijk wordt geregeld door applicatiebeheer van de afdeling WIZ.

De formele procedure waarmee autorisatie en registratie van gebruikers tot Suwinet plaatsvindt en gecontroleerd wordt verloopt als volgt:

Nieuwe medewerker

↓

Staf bepaalt aan de hand van de functieomschrijving welke autorisatie hij/zij krijgt.

↓

Betreffende teamleider geeft aan applicatiebeheer door wie de autorisatie tot SUWI-net moet krijgen en rekening houdend met de functie.

↓

Applicatiebeheer voert medewerker op en verleend gelet op de functie aan hem/haar de rol en de autorisatie.

↓

Er wordt een register / lijst van geautoriseerde medewerkers bijgehouden welke allemaal een geheimhoudingsverklaring hebben ondertekend.

↓

Maandelijks, tijdens regulier overleg ICB (Interne Controle Beveiliging), worden de accounts op actualiteit en volledigheid bekeken.

↓

Tevens wordt dan het gebruik van SUWI-net door de medewerkers door ICB gecontroleerd aan de hand van de maandelijks opgevraagde BKWI gebruikersrapportage.

↓

Deze monitor geeft eventueel voor ICB aanleiding tot nader onderzoek. Hiertoe zal dan door applicatiebeheer een specifieke rapportage bij BKWI worden opgevraagd.

↓

Bevindingen worden door ICB vastgelegd en door ICB zullen eventuele verdere acties worden uitgezet.

↓

Controle (het vervolg) hierop vindt plaats tijdens maandelijks ICB-overleg.

Als een gebruiker voor de eerste keer inlogt, dan is hij/zij verplicht (door Suwinet- Inkijk) het wachtwoord te wijzigen. In dit geval dient het wachtwoord:

- minimaal 8 tekens, waarvan in ieder geval één teken voorkomt uit elk van de onderstaande series:
  - 0123456789
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - abcdefghijklmnopqrstuvwxyz
  - ~!@#$%^&*()-_=+[]{}|;:,.<>/?
- mag niet gelijk zijn aan uw voornaam, uw achternaam of uw gebruikersnaam,
- mag niet gelijk zijn aan één van de laatste 5 eerder gekozen wachtwoorden,
- moet minimaal 3 tekens verschillen van een eerder gebruikt wachtwoord.

Wanneer het wachtwoord van een gebruiker verloopt (33 dagen niet gebruikt), verplicht Suwinet- Inkijk de gebruiker zijn/haar wachtwoord te veranderen.

Het gebruik van het account en wachtwoord is strikt persoonlijk. Geef je deze gegevens aan iemand anders en deze misbruikt deze informatie, dan staan jouw gegevens in de logbestanden.

Het BKWI*, de organisatie achter Suwinet- Inkijk rapporteert over het gebruik van de verschillende diensten op SUWINET aan de aangesloten partijen. Daartoe worden de activiteiten van SUWINET-gebruikers vastgelegd in logfiles.

Aan de hand van deze logfiles controleert het BKWI onder andere of:
-raadplegingen zijn gedaan buiten het klantenbestand,
-onevenredig veel zoekacties op 1 BSN zijn gedaan,
-iemand onevenredig veel raadplegingen doet,
-accounts zijn die niet of nauwelijks gebruik maken van Suwinet- Inkijk.

Sinds januari 2011 maken we gebruik van de monitor "gebruik Suwinet- Inkijk" van het BKWI.
Deze tool geeft snel inzicht in de stand van zaken over een aantal beveiligingsonderwerpen. Aan de hand van zeven normen uit het Normenkader Gezamenlijke elektronische Voorzieningen SUWI (GeVS) wordt getoetst of de beveiliging rondom Suwinet op orde is. Vier normen toetsen of de verantwoordelijkheden goed zijn verdeeld. Drie normen kijken of dat goed is geborgd in de organisatie
(Deze monitor en de verschillende rapportages zijn opgeborgen in de klapper Suwinet Inkijk, locatie kamer applicatiebeheer)

Civision SAM

Voor wie is *Civision SAM?*

Civision SAM biedt de klantmanagers en andere medewerkers alle informatie en ondersteuning, die nodig zijn om hun taken goed uit te voeren – van intake tot en met betaling en verantwoording, waarbij de uitstroom naar betaalde arbeid en een effectieve zorg vooropstaan.

Toegangsbeveiliging
Een door het afdelingshoofd/teamleider aangemelde medewerker krijgt toegang tot deze applicatie. Op basis van zijn/haar werkzaamheden krijgt hij/zij een rol toebedeeld binnen de applicatie. De autorisatie is beveiligd met naam en wachtwoord.
Het wachtwoord is minimaal zes karakters lang en bevat minimaal 1 cijfer.

Het beheer van de applicatie is in handen van applicatiebeheer.

Via mutatietabellen is inzichtelijk te maken wie welke wijziging heeft aangebracht in bepaalde velden. Zodat achteraf altijd is vast te stellen wat de feitelijke situatie op een bepaald moment was.

Liaan (zowel Liaan SR als Liaan Inlichtingenburo)

Voor wie is Liaan?

Deze applicatie wordt door de preventiemedewerkers en de sociale recherche gebruikt om fraudezaken te registreren en te verantwoorden naar het CBS.
Alleen zij hebben ook toegang tot deze applicatie.
Autorisatie en het beheer van de applicatie is in handen van applicatiebeheer.

Liaan herberekenen

Liaan herberekenen is een ondersteunende applicatie aan het primaire proces.
Op basis van een BSN worden correctieberekeningen of een klantprofiel opgesteld.
Autorisatie en het beheer van de applicatie is in handen van applicatiebeheer.

3.2 Uitgangspunten Informatiebeveiliging

Het Normenkader Informatiebeveiliging SUWI gegevensuitwisseling – de sociale dienst/afdeling sociale zaken kent de volgende uitgangspunten en aannames:
De Regeling SUWI dient als basis voor het bepalen van het beveiligingsniveau voor de uitwisseling van gegevens binnen SUWI;
Het beveiligingsniveau is bepaald op basis van de betrouwbaarheidseisen die staan beschreven in bijlage XIV van de Regeling SUWI.
Het normenkader is erop gericht er zorg voor te dragen dat de verwerking en uitwisseling van persoonsgegevens tussen de SUWI-organisaties voldoet aan de wettelijke eisen.
Informatiebeveiliging is een lijnverantwoordelijkheid.

Op grond van de Wbp kan een cliënt bij de afdeling WIZ inzage vragen in of correctie vragen van gegevens. Zulke verzoeken vereisen een zorgvuldige behandeling. Datzelfde geldt, in nog sterkere mate, bij de verstrekking van gegevens aan derden.
Naast deze privacyaspecten van de gegevensuitwisseling dienen ook algemene beveiligingsaspecten in acht te worden genomen. In artikel 13 Wbp staat namelijk bepaald dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer moet leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich brengen. Deze maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

De vraag welke beveiligingsmaatregelen door gemeenten c.q. de sociale diensten/afdelingen sociale zaken moeten worden genomen in het kader van de gegevensuitwisseling die plaatsvindt via het SUWINET dient te worden beantwoord aan de hand van de maatregelen omschreven in de zogenaamde risicoklassen. Het CBP gaat uit van de navolgende vier risicoklassen:

Aard van de gegevens Hoeveelheid van de gegevens	Persoonsgegevens	Bijzondere persoonsgegevens (Conform artikel 16 Wbp)	Financiële en/of economische persoonsgegevens
Lage complexiteit van verwerking en Weinig persoonsgegevens	Risicoklasse 0	Risicoklasse II	Risicoklasse II
Hoge complexiteit van verwerking en Veel persoonsgegevens	Risicoklasse I	Risicoklasse III	

Hoofdstuk 4. Beveiligingsorganisatie

4.1 Organisatorische infrastructuur voor informatiebeveiliging

College van B&W is verantwoordelijk voor het gebruik van persoonsgegevens door medewerkers van de gemeente.

Binnen het management van de afdeling WIZ is informatiebeveiliging in gang gezet en wordt beheerst. In deze paragraaf is aangegeven op welke wijze dit wordt uitgevoerd.

Functioneel is het afdelingshoofd WIZ de informatiemanager van de afdeling WIZ.
In deze hoedanigheid is hij verantwoordelijk voor informatiebeveiliging.

Op de afdeling WIZ zijn een drietal personen gezamenlijk verantwoordelijk voor de uitvoering van het beveiligingsbeleid en de daaruit voortvloeiende acties (verder aangeduid met driemanschap ICB).
Hiervoor is een driemanschap in het leven geroepen bestaande uit het afdelingshoofd, de interne controleur (T. Willems) en één van de applicatiebeheerders (E. Willems).
Gezamenlijk dragen zij zorg voor het opstellen en onderhouden van het beveiligingsplan.
Ook monitoren zij de uitvoering van de acties en aanbevelingen uit het beveiligingsplan.

De rol van Security Officer wordt binnen de afdeling Werk, Inkomen en Zorg vervuld door dhr. Harrie van Helvoirt, medewerker van de sector Bedrijfsvoering, afdeling Personeel Informatie Facilitair. De Security Officer zal 2 keer per jaar de beveiliging rondom Suwinet controleren en beoordelen en rapporteren aan het hoogste management.

4.2 Beveiliging van toegang door derden

Wanneer externen consultancy verrichten met behulp van ICT-toepassingen bij de afdeling WIZ worden deze "ingehuurd" via applicatiebeheer.
Het risico dat derden inzage hebben in persoonsgegevens is bij de afdeling WIZ voldoende ondervangen. Voordat applicaties met persoonsgegevens geopend kunnen worden, moet de gebruiker verschillende inlogcodes invoeren. Zonder login kan zelfs geen gebruik gemaakt worden van het gemeentelijke netwerk.
Externen worden altijd begeleid door applicatiebeheer. Werkzaamheden worden feitelijk gedaan door applicatiebeheer onder toezicht van de externen.

4.3 Uitbesteding

Alle data van de afdeling WIZ wordt opgeslagen op het netwerk van de gemeente Weert. Documenten staan fysiek op het netwerk, inputdata (het geen men invult in de schermen van de applicatie) wordt opgeslagen in databases. Fysieke dossiers worden na afloop van het werkproces gedigitaliseerd, voor zover nog nodig, en opgeslagen binnen de Decos database.

De beveiliging van de data bij de afdeling WIZ is deels uitbesteed.
Alle data wordt gebackuped, om bij dataverlies terug te kunnen vallen op de oorspronkelijke situatie. De back-upfaciliteit vindt deels buitenshuis plaats (Openline Smart ICT solutions).

Steeds meer toepassingen en informatie wordt ontsloten via het internet.
Het verkeer tussen het lokale netwerk en het internet wordt beveiligd met een firewall.
Het beheer van deze firewall wordt door een externe partij verzorgd (Kahuna).

Hoofdstuk 5. Classificatie en beheer van bedrijfsmiddelen

5.1 Classificatie van informatie

In deze paragraaf wordt aangegeven op welke wijze informatie binnen de afdeling WIZ is gecategoriseerd.

Binnen de afdeling WIZ wordt gewerkt met persoonsgegevens die aangemerkt kunnen worden als bijzondere persoonsgegevens zoals beschreven in artikel 16 Wbp. Omdat deze gegevens niet specifiek onderscheiden kunnen worden binnen de gegevensuitwisseling en gezien het grote aantal uitwisselingen, wordt de risicoklasse van de gegevens vastgesteld op een combinatie van II en III.

Logbestanden en de gebruikersadministratie bevatten persoonsgegevens van medewerkers. De gegevens die worden vastgelegd in deze bestanden worden vastgelegd in risicoklasse I.

Voor de afdeling Werk, Inkomen en Zorg van de gemeente Weert geldt dat de gemelde registraties als volgt worden gecategoriseerd.

Soort verwerking	Indeling in risicoklassen
Uitkeringenadministratie	**II/III**
Suwinet- Inkijk	**II/III**
Sociale recherche (frauderegistratiesysteem)	**II/III**

Om te voorkomen dat medewerkers van de dienst bij een eventuele crash van het netwerk gegevens over langere tijd kwijt zijn, worden dagelijks back-ups gedraaid van alle servers. Concreet betekent dit dat alle gegevens die zich op de servers bevinden (data, rapporten, beschikkingen etc.) elke avond worden opgeslagen. Het feitelijk uitvoeren van de back-ups wordt uitgevoerd door ICT. Het is onduidelijk welke afspraken er tussen ICT en de verschillende afdelingen van de gemeente zijn met betrekking tot herstel en prioritering.

Hoofdstuk 6. Beveiligingseisen ten aanzien van personeel

6.1 Beveiligingseisen bij aanname van personeel

Een zorgvuldige procedure bij indiensttreding kan de organisatie behoeden voor integriteitschendingen.
Een nieuwe medewerker moet niet alleen over de vakinhoudelijke kwaliteiten beschikken, maar ook betrouwbaar zijn. Door potentiële nieuwe medewerkers te "screenen" verkleint men de kans om "rotte appels" binnen te halen. Het screenen kan bijvoorbeeld door:
- het controleren van de juistheid van de doorgegeven persoonlijke gegevens;
- het doorvragen over het CV;
- het laten meenemen van originele exemplaren van diploma's;
- het controleren van referenties;
- het overleggen van een verklaring van goed gedrag.

Bij fraudegevoelige of andere kwetsbare functies is er zonder meer aanleiding om de integriteit van de sollicitant te onderzoeken bijvoorbeeld door het laten aanvragen van een

verklaring van goed gedrag (VOG). Als er een VOG wordt afgegeven betekent dit dat er geen voor de functie relevante strafbare gedragingen hebben plaatsgevonden.

De selectie van nieuw personeel dient te gebeuren door minimaal 2 personen die onbevooroordeeld zijn ten opzichte van de kandidaten.
In het sollicitatiegesprek komen de volgende onderwerpen aan bod:
- keuze voor de overheid;
- betekenis van het ambtenaar-zijn;
- specifieke risico's van de functie;
- van toepassing zijnde competenties;
- gedragscodes;
- ambtseed / integriteitverklaring;
- eventueel scholing gericht op weerbaarheid.

Vast personeel
Personeel dat in dienst is bij de gemeente valt direct onder het ambtenarenreglement. De Ambtenarenwet is recentelijk aangepast waardoor overheidswerkgevers verplicht zijn om een gedragscode op te stellen voor hun ambtenaren, de ambtseed of belofte te introduceren en integriteitbeleid te voeren. De Gemeente Weert beschikt over dit beleid, dit is terug te vinden op het Intranet van de gemeente Weert.

Elke nieuwe ambtenaar tekent sinds 2008 een integriteitverklaring, hierin geef je aan dat je alle zaken waarvan je weet of vermoedt dat ze een vertrouwelijk karakter hebben, geheim houdt.

Naast het ambtelijk personeel vraagt ook het aannemen van uitzendkrachten, stagiairs en ingehuurd personeel van bureaus om waarborgen. De organisatie moet nagaan tot welke, eventueel vertrouwelijke, informatie uitzendkrachten en stagiairs toegang hebben en of dit wenselijk is.
Er kan hen in ieder geval een geheimhoudingverklaring voorgelegd worden. Ook kan van hen gevraagd worden een VOG te overleggen. Het feit dat men (enige) werkzaamheden binnen de gemeente verricht is daarvoor voldoende.(zie: actiepunt 2)

6.2 Gebruikers van geautomatiseerde systemen

Applicatiebeheer van de afdeling WIZ instrueert de individuele gebruikers over correcte omgang met ICT-toepassingen.
Binnen de afdeling WIZ wordt met betrekking tot SUWINET een gebruikershandleiding beschikbaar gesteld aan alle nieuwe gebruikers.

Jaarlijks worden er door applicatiebeheer opfriscursussen voor de diverse geautomatiseerde toepassingen verzorgd.

Nieuwsbrieven en tips met betrekking tot het gebruik van bepaalde applicaties worden gedeeld met alle gebruikers. Dit wordt zowel via email als via de gemeentelijke pagina binnen grip op WWB bekend gemaakt.

Tijdens het inwerken door de naaste collega worden de nieuwe medewerkers in kennis gesteld van het gebruik van privacygevoelige informatie.
In welke situatie al dan niet informatie aan klanten en/of derden verstrekt mag worden, is ingegeven wat hierover in de WWB staat.

6.3 Reageren op incidenten en storingen

In deze paragraaf is aangegeven op welke wijze de afdeling WIZ incidenten die de beveiliging aantasten verwerkt en registreert.

Wanneer zich binnen de afdeling WIZ een storing voordoet wordt dit in eerste instantie gemeld bij applicatiebeheer. Deze beoordeeld of dit een applicatiegerelateerde of systeemtechnische melding is. In het eerste geval zal applicatiebeheer zelf de storing proberen op te lossen.
Een systeemtechnische melding wordt telefonisch doorgegeven aan de helpdesk ICT. Op de telefonische melding volgt altijd een mail. Deze mail wordt namelijk als registratie gebruikt in het helpdesksysteem van ICT.

De mail wordt altijd beantwoord met een call-nummer zo heeft applicatiebeheer ook een registratie. Als de storing/call uiteindelijk opgelost is ontvangt zowel de gebruiker als applicatiebeheer een mail.

Iedere medewerker binnen WIZ is bekend met deze werkwijze.

In een escalatieprocedure is voorzien. Het afdelingshoofd WIZ zal dan contact zoeken met het afdelinghoofd PIF (Personeel, Informatie en Facilitair), die het team ICT-services dan opdracht geeft tot het verrichten van bepaalde acties.

6.3.1 Rapporteren van onvolkomenheden in de software

Bij de afdeling WIZ is applicatiebeheer verantwoordelijk voor Civision SAM, SUWINET en de overige applicaties.
Bij eventuele problemen op software gebied zijn zij degene die als aanspreekpunt fungeren voor de medewerkers.

Applicatiebeheer beschikt over telefoonnummers van de diverse servicedesks en helpdesks van leveranciers en overheidsorganisaties.
Storingen, wensen en gebruikervragen kunnen zowel telefonisch als via de mail worden aangeleverd. Veelal krijg je hiervan een terugkoppeling via een call-nummer, zodat je de voortgang kunt volgen.

Bij PinkRoccade, de leverancier van Civision SAM, wordt een programmafout uiteindelijk op een meldingenlijst geplaatst.
Deze worden niet meteen opgelost maar zullen gebundeld worden opgelost. Dit kan in een patch op de software of met een nieuwe release.

Betreft het een storing in de besturingssoftware of in de communicatie, dan wordt zoals in hoofdstuk 6.3 beschreven ICT ingeschakeld.

6.3.2 Lering trekken uit incidenten

Er is binnen de afdeling WIZ geen apart softwarepakket dat fungeert als een registratiesysteem voor incidenten. ICT beschikt wel over een dergelijk tool.

Hoofdstuk 7. Fysieke beveiliging en beveiliging van de omgeving

7.1 Beveiligde ruimten

Deze paragraaf geeft inzicht in de wijze waarop de afdeling WIZ zich beschermd tegen ongeoorloofde toegang, schade en storingen.

De afdeling WIZ is zeer afhankelijk van ICT-voorzieningen voor het verrichten van de primaire processen. Uitval van deze voorzieningen heeft mede als risico dat bijstandsuitkeringen niet of niet tijdig uitbetaald worden.
Om de risico's te borgen worden alle servers, met daarop de data van de softwarepakketten, gesynchroniseerd. De servers bevinden zich in het gemeentehuis en een exacte omgeving bevindt zich op de gemeentewerf in een ander gebouw.
De servers en de toegang tot deze ruimtes is enkel toegestaan voor medewerkers van ICT. Door middel van het fysiek afsluiten van deze ruimten is ongeoorloofde toegang geborgd.

7.2 Fysieke beveiliging en toegang

Bij de afdeling WIZ is een deel van het gebouw toegankelijk voor publiek. Die zonder beperkingen te betreden zijn voor bezoekers.

De hoofdingang (bezoekersingang)

- Bezoek (zowel aangekondigd als onaangekondigd) dient zich te melden bij de receptie.
- Cliënten kunnen direct naar de juiste balie (WMO, Uitkering) gaan als de schuifdeuren open zijn.

De wachtruimten voor de balies en de spreekkamers is voor publiek vrij toegankelijk.
In de wachtruimten wordt door het afdelingshoofd opgetreden bij dreigende situaties.
Voor de afhandeling van dreigende situaties geldt het agressieprotocol.

In de spreekkamers is het meubilair gezekerd. De deuren zijn via aparte sloten beveiligd.

De personeelsingang en de werkruimten worden beveiligd door middel van een badgelezer.

Hoofdstuk 8. Beheer van communicatie- en bedieningsprocessen

8.1 Bedieningsprocedures en verantwoordelijkheden

In deze paragraaf is beschreven welke procedures er gelden binnen de afdeling WIZ op het gebied van aanpassingen, incidenten en functiescheiding op ICT-gebied.

Bijna alle werkprocessen die gebruikt worden in het primaire proces van de afdeling WIZ, zijn gedocumenteerd met behulp van werkinstructies en werkbeschrijvingen.
Wijzigingen in deze processen leiden tot gewijzigde instructies. Op deze manier hebben de medewerkers van de afdeling WIZ altijd de beschikking over bijgewerkte instructies en beschrijvingen om de werkzaamheden uit te voeren.

De implementatie van nieuwe releases wordt in samenspraak met ICT uitgevoerd. In overleg met de afdeling WIZ wordt een datum geprikt om tot feitelijke installatie over te gaan. Dit zal eerst in een testomgeving worden uitgevoerd. Na een succesvolle test wordt dezelfde procedure herhaald maar dan in de productieomgeving.
Dit geldt voor alle primaire applicaties (Civision SAM, Liaan)

Wanneer op ICT gebied veranderingen plaatsvinden worden de medewerkers van de dienst daarover in kennis gesteld. Bij kleinere ingrepen via de mail, bij projecten met een grotere impact via het afdelingshoofd van de afdeling WIZ.

Enkel medewerkers van de ICT zijn bevoegd om wijzigingen in de ICT-infrastructuur aan te brengen. Op deze manier wordt voorkomen dat op verschillende plaatsen binnen de organisatie wijzigingen plaatsvinden en kunnen de zaken beheerst worden.

Iedere medewerker van de afdeling WIZ heeft enkel toegang tot ICT-voorzieningen die noodzakelijk zijn voor de uitoefening van zijn/haar werkzaamheden.
Er is een duidelijke functiescheiding.
Per functionaris verschillen, indien van toepassing, de autorisaties. Op deze manier wordt misbruik van voorzieningen tegengegaan.

Achteraf vindt er controle plaats op het gebied van de rechtmatigheid van de primaire processen. Deze controle wordt feitelijk uitgevoerd door applicatiebeheer in samenspraak met de kwaliteitsmedewerker WIZ.

8.2 Systeemplanning en acceptatie

Aangegeven wordt op welke manier nieuwe patches en releases worden geïmplementeerd.

Bij ICT wordt periodiek bekeken of de capaciteit van de verschillende servers van de gemeente nog voldoende is. De medewerkers van de afdeling WIZ hebben in deze geen rol.

Nieuwe releases en updates worden meteen in de testomgeving geïnstalleerd, en pas na een test vrijgegeven voor productie.
Acceptatie gebeurd zowel door applicatiebeheer als door gebruikers die vooraf benaderd zijn om de nieuwe release te beoordelen. Op basis van hun werk/discipline worden gebruikers benaderd om de geboden oplossingen van de leverancier te testen.

Hoofdstuk 9. Toegangsbeveiliging

9.1 Beleid ten aanzien van toegangsbeveiliging

Aangegeven wordt welke richtlijnen met betrekking tot toegangsbeveiliging bij het team zijn gedefinieerd.

Binnen de afdeling WIZ is vastgelegd dat enkel personen die binding hebben met de primaire processen toegang krijgen tot SUWINET en de overige applicaties. Ondersteunende afdelingen hebben in principe geen toegang tot SUWINET. In het kader van de informatievoorziening ontvangt iedere medewerker enkel autorisaties voor de voor hem belangrijke applicaties.

9.2 Registratie van gebruikers

Nieuwe medewerkers ontvangen via ICT binnen afgesproken termijnen een userid, wachtwoord en gebruikersprofiel.
De afdeling WIZ geeft in eerste instantie door aan ICT welke bevoegdheden een betreffende medewerker heeft, waarna de noodzakelijke applicaties aan het gebruikersprofiel worden gekoppeld.

9.3 Speciale bevoegdheden

Er zijn bij de afdeling WIZ 2 medewerkers (applicatiebeheerders) met speciale bevoegdheden aanwezig.
Dit zijn aparte netwerkprofielen die door ICT worden verstrekt.

9.4 Beheer gebruikerswachtwoorden

Om te voorkomen dat medewerkers gedurende zeer lange tijd hetzelfde wachtwoord gebruiken, dienen zij na een afgesproken periode het netwerkwachtwoord te wijzigen. Dit om misbruik van de wachtwoorden te voorkomen.

Op applicatieniveau geldt dat wanneer het wachtwoord van een gebruiker verloopt, verplicht Suwinet de gebruiker zijn/haar wachtwoord te veranderen. Dit geldt niet voor Civision SAM of de Liaan applicaties.

Na 3 mislukte inlogpogingen wordt de gebruiker geblokkeerd, dit geldt voor elke applicatie.

9.5 Verantwoordelijkheden van gebruikers

Effectieve beveiliging vereist de medewerking van de gebruikers. Zij dienen daarom te worden gewezen op hun verantwoordelijkheid voor het handhaven van effectieve toegangsbeveiliging, vooral met betrekking tot het gebruik van wachtwoorden en de beveiliging van gebruikersapparatuur. In het werkoverleg en op Intranet wordt hierover gecommuniceerd.

9.6 Gebruik van wachtwoorden

Medewerkers van de afdeling WIZ zijn zelf verantwoordelijk voor het voorkomen van ongeautoriseerde toegang. Dit betekent dat zij op een verantwoorde wijze om moeten gaan met wachtwoorden en registratie daarvan. Kenbaar gemaakt is dat wachtwoorden strikt persoonlijk zijn en niet uitgewisseld moeten worden tussen collega's (uitzonderlijke noodsituaties uitgesloten).

Bij het opstarten van elke pc is de gebruiker verplicht een userid en wachtwoord in te geven alvorens van het gemeentelijke netwerk gebruik gemaakt kan worden. Om vervolgens de afzonderlijke applicaties te starten moet ook per applicatie een userid en wachtwoord ingevoerd worden.

Periodiek (Suwinet- Inkijk) verschijnt de melding dat het wachtwoord verlopen is en een nieuw wachtwoord moet worden ingevoerd. Dit geldt niet voor Civision SAM of de Liaan applicaties

9.7 Onbeheerde gebruikersapparatuur

Voorkomen dient te worden dat tijdelijk onbeheerde gebruikersapparatuur ongeoorloofd gebruikt wordt om toegang te krijgen tot persoonsgegevens.

In principe is geen enkele computer toegankelijk voor klanten of derden. Enkel de medewerkers van de afdeling WIZ zijn instaat tot het gebruik hiervan binnen het domein inkomen en zorg. In de publiekstoegankelijke wachtruimte zijn geen computers opgesteld.

Op dit moment wordt bij afwezigheid van de medewerker, automatisch na een vastgestelde periode een schermblokkade met wachtwoord toegepast. Deze is ook direct door de gebruiker in te stellen bij het verlaten van de werkplek (Toets Windowsvlag + L)

Er zijn hieromtrent geen concrete afspraken gemaakt, maar het verdient aanbeveling om deze mogelijkheid van schermbeveiliging toe te passen, vooral voor consulenten die gesprekken voeren in de spreekkamer. (zie: aanbevelingen)

Hoofdstuk 10. Continuïteitsmanagement

Binnen de afdeling WIZ is een proces gestart dat er op gericht is om calamiteiten en incidenten tot een aanvaardbaar niveau te beperken. Welke concrete maatregel worden genomen staat in deze paragraaf.

10.1 Aspecten van continuïteitsmanagement

Het algemeen gebruik en acceptatie van internettoepassingen kan als consequentie hebben dat we 24*7 uur bereikbaar zijn voor de burger of ketenpartners.
Deze ontwikkeling heeft ook consequenties voor het beheer van systemen.

Onderhoud en updates worden normaliter buiten kantoortijden uitgevoerd.
Als de kantoortijden dus oprekken kunnen de onderhoud- en updatewerkzaamheden in het gedrang komen.

Storingen en bedreigingen kunnen de gehele dag plaatsvinden op de ICT-omgeving.

Binnen de afdeling WIZ is het primaire proces beveiligd tegen uitval van het ICT-systeem.

De backup is hier een onderdeel van.
Elke weekend wordt er een volledige backup gedraaid, elke werkdag incremental (dus alleen de veranderingen t.o.v. de vorige)
Weekbackups worden een maand bewaard, maandbackups worden een jaar bewaard. Jaarbackups worden altijd bewaard.

Full backups worden gearchiveerd. Elke maand wordt er een maandtape gemaakt.
Daarnaast worden er jaartapes gemaakt. We kunnen 4 jaar terug

Op het gebied van calamiteiten zoals brand, bommeldingen etc. is het calamiteitenplan van kracht. Uitwijk is hier een onderdeel van.
In de huidige situatie draait een volledige mirror tussen de Beekstraat en de Werf. Op het moment dat 1 van de 2 uitvalt, neemt de andere het direct over. De gebruiker merkt daar niks van.
Het is een zogenaamde synchrone mirror. Elke wijziging die op de Beekstraat wordt weggeschreven, is binnen een seconde ook weggeschreven op de Werf.

In de nieuwe situatie (samenwerking met Venlo en Roermond) gaat de situatie er anders uitzien.

De verdergaande digitalisering van klantdossiers binnen Decos valt buiten dit beveiligingsplan.

Hoofdstuk 11. Naleving

11.1 ICB (interne controle beveiliging)

Binnen de afdeling WIZ is een driemanschap ICB (interne controle beveiliging) ingesteld bestaande uit:
het afdelingshoofd, Kees Joosten, de beleidsmedewerker IC, Ton Willems en een applicatiebeheerder, Edwin Willems.

Deze hebben elke maand overleg over informatiebeveiliging. Tijdens dit overleg wordt het BKWI rapport, wat elke maand door de applicatiebeheerder (Edwin Willems) wordt opgevraagd, besproken. De analyse / bevindingen worden in een verslag / rapport vastgelegd. Evident dat daarnaast op landelijke en regionale incidenten alert en adequaat gereageerd wordt.

In opdracht van de VNG heeft de IBD (Informatiebeveiligingsdienst voor gemeenten) een baseline informatiebeveiliging gemeenten ontwikkeld (BIG).
Dit basisnormenkader informatieveiligheid voor gemeenten stelt ons in staat om te meten of we de basis op orde hebben en of we voldoen aan normen en wettelijke voorschriften op het gebeid van informatiebeveiliging.

Dit basisnormenkader is omgezet in een scorematrix* (monitor gebruik Suwinet-Inkijk).
Deze scorematrix wordt 2 keer per jaar geëvalueerd door het driemanschap.
Samen met de rapportages gebruik Suwinet services en de door applicatiebeheer geregistreerde opmerkingen vormt dit de basis voor het ICB overleg.

(*De scorematrix is als losse bijlage toegevoegd)

Hoofdstuk 12 Conclusies en aanbevelingen.

12.1 Conclusie

Het plan ligt er nu. Het verantwoordelijke management heeft het voorliggende informatiebeveiligingsplan beoordeeld op volledigheid en juistheid.

Het plan wordt voorgelegd aan het college van B&W, voor bestuurlijke aandacht en vaststelling van het informatiebeleid.

Om informatiebeveiliging onder de aandacht te blijven houden moet dit beleid, en de daaruit voortvloeiende activiteiten, uitgedragen en verdedigd worden.
De mensen die verantwoordelijk zijn voor de informatiesystemen en -beveiliging zullen moeten nadenken over de wijze van beveiliging, al voordat ze persoonsgegevens gaan verzamelen.
De beveiliging van persoonsgegevens binnen een organisatie moet gedurende de gehele levensduur van een informatiesysteem punt van aandacht zijn, van het allereerste ontwerp tot aan het onomkeerbaar wissen van het laatste back-upbestand na afloop van de bewaartermijn.

De kwaliteit van de Informatiebeveiliging valt of staat met de mensen die werken op de afdeling. Het is van groot belang dat iedereen weet waarom en welke spelregels er zijn.

Afkortingen en begrippenlijst

Code voor informatiebeveiliging	De Code voor Informatiebeveiliging beschrijft in 11 hoofdstukken normen en maatregelen, die van belang zijn voor het realiseren van een afdoende niveau van informatiebeveiliging. De Code wordt uitgebracht door het Nederlands Normalisatie-instituut.
Afdeling WIZ	Afdeling Werk, Inkomen en Zorg
DT	Directie team gemeente Weert
Regeling SUWI	Wet structuur uitvoeringsorganisatie werk en inkomen
SZW	Ministerie van Sociale Zaken en Werkgelegenheid
Divosa	is de Nederlandse vereniging van gemeentelijke managers op het terrein van participatie, werk en inkomen
Wbp	Wet bescherming persoonsgegevens
CBP	College bescherming persoonsgegevens
afdeling PIF	Personeel, Informatie en Facilitair
BKWI	Bureau Keteninformatisering Werk & Inkomen. Het BKWI ondersteunt en ontwikkelt met en voor ketenpartners ICT-oplossingen op functioneel en technisch gebied

Bijlagen

1) Tien gouden regels voor het gebruik van informatie, informatiesystemen en netwerken.

2) Integriteitsverklaring.

3) Gebruik SUWINET binnen werk.kom(samenwerkingsverband)

4) Autorisatiematrix

- Scorematrix Monitor gebruik Suwinet –Inkijk.

Bijlage 1) Tien gouden regels: voor het gebruik van informatie, informatiesystemen en netwerken.

Wij vragen even om jouw aandacht!

Afhankelijk van jouw functie heb jij toegang tot diverse informatiesystemen binnen de afdeling WIZ. Wij willen je erop attenderen dat het gebruik van deze systemen verbonden is aan een aantal verplichtingen. Met deze *tien gouden regels* vatten wij de belangrijkste hiervan samen. Wij verzoeken je deze goed door te lezen omdat zij deel uitmaken van je functie binnen de afdeling WIZ.

1. **Wachtwoorden zijn strikt persoonlijk**
Je wachtwoorden zijn strikt persoonlijk en dienen uitsluitend door jou gebruikt te worden om toegang te krijgen tot de betreffende systemen. Geef je wachtwoord dus niet aan derden of een collega en bewaar ze op een *veilige* plek, dus *niet* in je agenda of op een geel briefje!

2. **Melden van beveiligingsincidenten**
Softwarematige beveiligingsincidenten meld je zo snel als mogelijk bij applicatiebeheer. Voorbeelden van een dergelijk incident is een virusmelding op het systeem.
Een ander beveiligingsincident bijvoorbeeld een deur die op slot had moeten zijn maar niet op slot is, meld je bij je werkleider/afdelingshoofd.

3. **Geheimhoudingsplicht**
Binnen de sociale dienst/afdeling sociale zaken wordt veel met persoonsgegevens gewerkt. Voor het werken en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (Wbp). In de wet SUWI en in de CAO zijn daarom geheimhoudingsbepalingen opgenomen die inhouden dat je de persoonsgegevens niet verder bekend mag maken dan voor de uitoefening van je functie noodzakelijk is. Dit betreft persoonsgegevens die vanuit je werkzaamheden bekend worden, evenals overige informatie waarvan je weet of redelijkerwijze kunt vermoeden dat geheimhouding verplicht is.

4. **Gedragscode Internet- en e-mailgebruik**
Er is geen gedragscode voor Internet- en e-mailgebruik die aangeven hoe de medewerkers van de afdeling WIZ behoren om te gaan met Internet en e-mail op de werkplek.

E-mail verkeer geldt inmiddels als algemeen geaccepteerde correspondentie, gelijk aan brieven. E-mails kunnen, mits de betrouwbaarheid van het e-mail adres voldoende is aangetoond, gelden als bewijsstuk.

Bovenstaande alinea is enkel van toepassing voor e-mail verkeer tussen de afdeling WIZ en instanties!
Contactpersonen kunnen door middel van het verzenden van e-mail op een snelle manier informatie uitwisselen over individuele klanten.
E-mail verkeer tussen klanten en medewerkers van de afdeling WIZ wordt ten zeerste afgeraden omdat deze correspondentie niet centraal wordt geregistreerd (voorzetting huidige werkwijze).
E-mails die klanten versturen aan hun contactpersoon worden niet gezien als bewijsstuk.

5. Kennisnemen van het informatiebeveiligingsbeleid

Het binnen de afdeling WIZ geldende informatiebeveiligingsbeleid en de bijbehorende richtlijnen, instructies en protocollen zijn op iedereen in onze organisatie van toepassing. Vraag je leidinggevende voor meer informatie hierover.

6. Gegevensverstrekking aan derden via de telefoon

Het uitgangspunt is dat er niet aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen. Dat betekent dat er ook geen telefonische informatie over klanten wordt verstrekt aan personen of instanties die beweren namens de betrokkene te bellen. Vragen dienen schriftelijk bij de afdeling WIZ te worden ingediend. Enkel in uitzonderlijke gevallen kan informatie verstrekt worden aan derden, indien de identiteit van deze voldoende vastgesteld kan worden (bijvoorbeeld door middel van terugbellen via een centraal telefoonnummer) en een schriftelijk verzoek tot informatie **niet** mogelijk is.

7. Clear desk / clear screen policy

De vertrouwelijke omgang met persoonsgegevens houdt o.a. in dat elke werkplek zodanig is ingericht, dat onbevoegde niet in jou afwezigheid aan deze gegevens kunnen komen. Dat betekent dat jij je werkstation bewust dient te vergrendelen met behulp van de screensaver (toetscombinatie (Windowsvlag + L) wanneer jij je werkplek verlaat. Ook mogen geen vertrouwelijke gegevens, zoals dossiers of verslagen, onbeheerd op je bureau/spreekkamer of in een niet afsluitbare kast blijven liggen.

8. Geen vertrouwelijke gegevens in de prullenbak

De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen de afdeling WIZ. Ook het vernietigen van deze gegevens moet op een veilige manier plaats vinden. Daarom zijn er speciale gekenmerkte papiercontainers binnen de afdeling WIZ aanwezig (de blauwe containers). Maak hiervan gebruik en stop vertrouwelijke gegevens *nooit* in de prullenbak of in een bak op je kamer die bestemd is voor oud-papier.

9. Aanspreken van onbekende personen

Ben je al een keer in de situatie geweest, dat je iemand binnen het gebouw tegenkwam, waar officieel geen publiek zonder begeleiding mag komen en je niet wist wie deze persoon was en wat zij daar te doen had? Spreek deze persoon aan, stel jezelf voor en vraag, wat hij of zij hier komt doen. Nieuwe collega's, uitzendkrachten of ander ingehuurd personeel stellen het op prijs om aangesproken te worden en op deze manier contacten te kunnen leggen. Echter, personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Wijs hun beleeft, maar duidelijk, de weg naar het publieke gedeelte van het gebouw en – belangrijk – begeleidt ze daar naartoe.

10. Haast, stress, werkdrukte vs. informatiebeveiliging

Informatiebeveiliging krijg je niet gratis – het kost je energie en werkt vaak tegen je als je haast hebt en de werkdrukte hoog is. Echter, informatiebeveiliging is uitermate belangrijk voor je werk binnen de afdeling WIZ en hoort bij de professionele en bekwame uitvoering van het werk. Neem het daarom zeer serieus – je cliënten vertrouwen erop!

Bijlage 2) Integriteitsverklaring

GEMEENTE WEERT

Integriteitverklaring

De gemeente Weert wil een integere organisatie zijn die zich inzet voor de belangen van de gemeente Weert en het vertrouwen heeft van de burgers. De gemeente Weert heeft als overheidsinstelling een voorbeeldfunctie in de maatschappij.

Daartoe verklaar ik als ambtenaar van de gemeente Weert het volgende:

- *ik zal de gerechtigheid dienen;*
- *ik zal trouw zijn aan de grondwet en aan de overige wetten van het rijk;*
- *ik zal me inzetten voor het algemeen belang van de gemeente Weert en werken voor alle burgers van de gemeente Weert;*
- *ik zal onpartijdig handelen en de democratische beginselen en procedures respecteren;*
- *ik ben loyaal ten opzichte van de bestuursorganen van de gemeente Weert en het door die bestuursorganen vastgestelde beleid;*
- *ik zal van de overheidsmacht die mij is toevertrouwd geen misbruik maken;*
- *ik zal zorgvuldig omgaan met gemeentelijke informatie en eigendommen;*
- *ik zal de geloofwaardigheid van het ambt niet schaden;*
- *ik zal het vertrouwen, dat de burger in mij mag stellen, niet beschamen;*
- *ik zal mij een zelfstandig oordeel vormen over de morele juistheid van mijn handelen.*

Dat verklaar ik,

te Weert

_____ _____

Datum *Naam en handtekening*

Bijlage 3)

Gebruik Suwinet binnen Werk.Kom (aanvulling op het gemeentelijke informatiebeveiligingsplan)

Nederweert, Weert en de Risse Groep hebben de re-integratie, detachering en werkgeversbenadering sinds april 2013 gezamenlijk vorm gegeven onder de naam Werk.Kom. Het samenwerkingsverband is gevestigd aan de Risseweg 8 in Weert. Sanne Timmermans is als consulent Intake & Diagnose, in dienst van de gemeente Nederweert, tewerkgesteld binnen Werk.Kom. Vanuit haar vorige functie is ze bekend met de werking en het gebruik van Suwinet. Sanne Timmermans blijft Suwinet ook binnen Werk.Kom gebruiken, maar de autorisatie wordt beperkt tot de rol GSD. Het is namelijk de bedoeling dat Sanne voor Werk.Kom op BSN enkel kan nakijken of door gemeente Nederweert en/of Weert bij uitstroom de uitkeringen zijn beëindigd. De werkzaamheden zijn noodzakelijk voor een goede uitvoering van de Wet werk en bijstand door Sociale Zaken. Aan de hand van deze handeling wordt bepaald wat de netto uitstroom is en of vervolgacties op het gebied van de Wet werk en bijstand noodzakelijk zijn (waaronder een re-integratietraject). De autorisatie is verstrekt in overleg met Weert (Edwin Willems), Nederweert (Harold van der Haar), Toine Witters (manager Werk.Kom) en BKWI (Ted Strik). De security-officers van Nederweert en Weert zijn geïnformeerd en Sanne Timmermans weet dat zij de enige is die binnen Werk.Kom gebruik mag maken van Suwinet en dat de raadplegingen alleen te maken mogen hebben met het omschreven doel.

Weert, 12 september 2013

Burgemeester en wethouders van Weert,
Namens deze,
Het hoofd van de afdeling Werk, Inkomen en Zorg

Bijlage 5) Extract uit de autorisatiematrix

Toegangsrechten voor SUWINET-INKIJK

Code	*Rol*	*Rol Civision SAM*
R1043	Belastingdienst	Consulent I&Z
R1272	Fraude Vorderingen	Preventie, Consulent T&V
G002	B&O	Consulent I&Z, Consulent A&W
G003	UWVWb	Iedereen
G004	FSK	Consulent I&Z

GEMEENTE WEERT

De heer Inspectie SZW
drs. J.W.T.M. Urselmann
Postbus 90801
2509 LV DEN HAAG

Weert, 9 februari 2015

Onderwerp : Conceptverslag van bevindingen onderzoek Veilig gebruik Suwinet
Ons kenmerk : 024627

Beste meneer drs. J.W.T.M. Urselmann,

Wij hebben uw conceptverslag van bevindingen Veilig gebruik Suwinet gelezen. In uw conceptverslag geeft u aan dat de gemeente Weert aan 3 van de 7 normen nog niet voldoet. Dit is voor de gemeente Weert aanleiding geweest om deze 3 normen opnieuw te bezien. Wij hebben uw reactie als aanbeveling opgevat.
In de bijlage treft u de uitgebreide reactie aan en de maatregelen die wij daartegen genomen hebben.

Ik ga ervan uit dat u onze reactie en de genomen maatregelen overneemt in het definitieve verslag voordat dit gepubliceerd wordt.

Mocht u onze reactie op de 3 punten als ontoereikend beoordelen en wij in uw ogen nog niet voldoen aan de eisen van Veilig gebruik Suwinet zouden wij dit graag vernemen met daarbij een nieuwe aanbeveling.

Met vriendelijke groet,
burgemeester en wethouders,

M.H.F. Knaapen
gemeentesecretaris

A.A.M.M. Heijmans
burgemeester

Bijlage(n) : 1

Wilhelminasingel 101
Correspondentie: Postbus 950, 6000 AZ Weert
Telefoon: 14 0495 of (0495) 57 50 00 - E-mail: gemeente@weert.nl
Website: www.weert.nl - Twitter: www.twitter.com/gemeenteweert

Overleg : Interne Controle Beveiliging
Datum: 28-01-2015
Deelnemers: Kees Joosten, Edwin Willems, Ton Willems

Agendapunt: conceptverslag van bevindingen van het onderzoek naar het veilig gebruik van Suwinet over 2014 opgesteld door Inspectie SZW.

Het verslag geeft voor 7 geselecteerde normen aan of wij als gemeente hieraan voldoen. Op 4 van de 7 normen wordt een voldoende gescoord. De andere 3 normen zijn besproken. Het betreft:

Norm 2.3
De Security Officer beheert en beheerst beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd.

De Security Officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status en controleert dat de beveiliging van de Suwinet maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet.

De Security Officer rapporteert rechtstreeks aan het hoogste management.

Bevinding Inspectie SZW

- Niet is aangetoond dat de Security Officer minimaal 2 keer per jaar de beveiliging rondom Suwinet controleert en beoordeelt en daarover rapporteert aan het hoogste management.
- Er is geen rapportage van de Security Officer aan het hoogste management geweest.
- Het afdelingshoofd WIZ is tevens Security Officer wat mogelijk belangenverstrengeling met zich meebrengt.

Reactie
We hebben de bevinding op gevat als een aanbeveling die we hebben overgenomen.
Maatregel:
het afdelingshoofd WIZ (sector Inwoners) Kees Joosten en tevens Security Officer zal zijn rol als Security Officer overdragen aan een medewerker van de sector Bedrijfsvoering, dhr. Harrie van Helvoort, Adviseur Informatievoorziening. De nieuw benoemde Security Officer zal de rapportage voor zijn rekening nemen.
De benoeming zal middels een collegevoorstel bekrachtigd worden.

Norm 13.1
De Suwi-partij autoriseert en registreert de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure waarin is opgenomen:

- Het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie/taken;
- Het uniek identificeren van elke gebruiker tot één persoon;
- Het goedkeuren van de aanvraag voor toegangsrechten door de manager of een gemandateerde;
- Het tijdig aanpassen of wijzigen van de autorisatie bij functiewijziging of vertrek;
- Het benaderen van de Suwi-databestanden door gebruikers mag alleen plaatsvinden via applicatieprogrammatuur (tenzij sprake is van calamiteiten).

Bevinding Inspectie SZW
Er is geen formele procedure waarmee autorisatie en registratie van gebruikers tot Suwinet plaatsvindt en wordt gecontroleerd.

Reactie
Er is geen formele procedure vastgelegd. Dit is een verbeterpunt en deze omissie zal z.s.m. worden hersteld.
De volgende procedure zal worden geformaliseerd en vastgesteld.

Nieuwe medewerker

↓

Het afdelingshoofd bepaalt aan de hand van de functieomschrijving in overleg met zijn staf welke autorisatie de nieuwe medewerker krijgt.

↓

Het afdelingshoofd geeft aan applicatiebeheer door wie de autorisatie tot SUWI-net moet krijgen.

↓

Applicatiebeheer voert medewerker op en verleent afhankelijk van de functie aan de nieuwe medewerker de rol en de autorisatie.

↓

Er wordt een register / lijst van geautoriseerde medewerkers bijgehouden welke allemaal een geheimhoudingsverklaring hebben ondertekend.

↓

Maandelijks, tijdens regulier overleg ICB (Interne Controle Bevelliging), worden de accounts op actualiteit en volledigheid gecontroleerd.

↓

Tevens wordt dan het gebruik van SUWI-net door de medewerkers door ICB gecontroleerd aan de hand van de maandelijks opgevraagde BKWI gebruikersrapportage.

↓

Deze monitor geeft eventueel voor ICB aanleiding tot nader onderzoek. Hiertoe zal dan door applicatiebeheer een specifieke rapportage bij BKWI worden opgevraagd.

↓

Bevindingen worden door ICB vastgelegd en door ICB zullen eventuele verdere acties worden uitgezet.

↓

Controle (het vervolg) hierop vindt plaats tijdens maandelijks ICB-overleg.

Deze procedure zal worden geformaliseerd en ter vaststelling worden voorgelegd aan de Security Officer.

Norm 13.5
De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats.

- Interne controle op rechten en gebruik van Suwinet
- Analyseren van de van het BKWI verkregen informatie over het gebruik van Suwigegevens.

Bevinding Inspectie SZW
- Er worden geen schriftelijke rapportages gemaakt over het gebruik van Suwinet.
- Er zijn geen specifieke rapportages opgevraagd.

Reactie
Tot op heden worden specifieke rapportages enkel opgevraagd als daar aanleiding toe is. Wij controleren op (on)juist gebruik van Suwinet maar de bevindingen worden niet vastgelegd. Ook deze bevinding vatten we op als een aanbeveling, en nemen wij over.
Maatregel:
Vanaf nu wordt elke maand door de applicatiebeheerder (Edwin Willems) een BKWI rapport opgevraagd. De analyse / bevindingen zullen in een verslag / rapport worden vastgelegd. Voor 2015 zijn elke maand overlegmomenten ingepland waarin dan o.a. de vastgelegde bevindingen besproken worden. Op landelijke en regionale incidenten zullen we alert zijn en adequaat reageren.